



**1. Datos Generales de la asignatura**

<b>Nombre de la asignatura:</b>	<b>Cómputo Forense</b>
<b>Clave de la asignatura:</b>	<b>CSD-2405</b>
<b>SATCA<sup>1</sup>:</b>	<b><u>2-3-5</u></b>
<b>Carrera:</b>	<b>Ingeniería en Sistemas Computacionales</b>

**2. Presentación**

**Caracterización de la asignatura**

Esta asignatura aporta al perfil de egreso del(la) Ingeniero(a) de Sistemas Computacionales:

- Implementa aplicaciones computacionales para solucionar problemas de diversos contextos, integrando diferentes tecnologías, plataformas o dispositivos.
- Coordina y participa en equipos multidisciplinarios para la aplicación de soluciones innovadoras en diferentes contextos.
- Administra software para apoyar la seguridad de las organizaciones cumpliendo con estándares de calidad.
- Evalúa tecnologías de hardware para soportar aplicaciones de manera efectiva.

Desde que apareció Internet, uno de sus principales objetivos está relacionado con su uso en las empresas y otras instituciones no comerciales. De hecho, la primera red de computadoras llamada “Arpanet” (Advanced Research Projects Agency Network) fue creada a petición del Departamento de Defensa de Estados Unidos como medio de comunicación para los diferentes organismos del país. De ahí en adelante sus beneficios se multiplicaron hasta lo que es ahora: una enorme plataforma que nos permite guardar y buscar datos, además de comunicarnos con cualquier empresa, sin importar la ubicación que posea en el mapa.

Sin embargo, tan importante como conocer sus beneficios es también entender los riesgos inherentes a la seguridad, cuando se implementa esta tecnología.

De acuerdo con algunas empresas de investigación, la seguridad de la información seguirá siendo una preocupación ejecutiva durante, al menos, los próximos cinco años, debido a las nuevas olas tecnológicas que modificarán las medidas de seguridad existentes.

Precisamente, con el objetivo de reducir en porcentaje este problema, es que aparece una nueva modalidad llamada “Informática Forense”, o “Cómputo Forense”, que permite la solución de conflictos tecnológicos relacionados con seguridad informática y protección de datos.

<sup>1</sup> Sistema de Asignación y Transferencia de Créditos Académicos



La presente asignatura contiene temas que le ayudarán al estudiante adquirir, tratar, y preservar evidencias digitales, mediante herramientas especializadas del cómputo forense, que le permitan entre otras cosas, minimizar daños causados por los criminales o intrusos, dar seguimiento y procesamiento judicial a los casos criminales empleando normas vigentes de cómputo forense, así como desarrollar medidas que le permitan prevenir casos similares.

Es una asignatura que pretende brindar al estudiante conocimientos metodológicos, y legales, así como también el estudio de distintas herramientas que le permitan indagar y recolectar evidencia de delitos informáticos cometidos en la organización.

El cómputo forense, es una asignatura diferente a las demás del Módulo de Especialidad de la carrera de Ingeniería en Sistemas Computacionales ya que, en ella, se facilitan conocimientos para analizar discos duros, dispositivos móviles, memorias USB, BIOS, archivos, carpetas, información electrónica, MAC address, logs de seguridad, IPs, redes, software, credenciales de autenticación, agendas electrónicas, dispositivos GPS, impresoras, entre otros.

Se relaciona con las siguientes asignaturas: Seguridad de la Infraestructura Tecnológica, Estándares de Ciberseguridad y Tópicos de Ciberseguridad, mismas que pertenecen al Módulo de especialidad de dicha carrera, con los temas: Seguridad Perimetral, Seguridad en Dispositivos Móviles e IoT, Herramientas de Pentesting, y Aplicación de Dominios de Ciberseguridad.

### **Intención didáctica**

El cómputo forense es una asignatura dividida en cuatro temas importantes, los cuales son: Introducción, Herramientas, Metodología y Análisis documental del Cómputo Forense.

En ellas se pretende brindar conocimiento de tal forma que el estudiante pueda adquirir conocimientos y habilidades para utilizar herramientas teórico – prácticas que le permitan obtener evidencia digital de los delitos cometidos a través de sistemas informáticos, que puedan ser utilizadas en un marco legal.

En la unidad uno se consideran temas básicos de la asignatura, también se presenta la terminología relacionada al cómputo forense, las áreas de aplicación, la clasificación de delitos informáticos y los dispositivos que son susceptibles al cómputo forense.

En la unidad dos se abordan temas sobre el uso de herramientas que le permitan al estudiante, recolectar evidencias, monitorear y controlar equipos de cómputo, marcar documentos, y realizar revisiones minuciosas del hardware involucrado en delitos informáticos. Se recomienda abordar herramientas que permitan la clonación de datos,



análisis de discos duros, de archivos, de internet, de correos electrónicos de dispositivos móviles entre otras herramientas del cómputo forense.

En la unidad tres, Metodología del cómputo forense, se considera conocer la metodología del cómputo forense y aplicarla a un caso práctico del contexto, considerando la identificación del hecho delictivo, preparación de herramientas y técnicas, adquisición de evidencias digitales, preservación de la escena física y digital, análisis e interpretación de evidencias y presentación de resultados a fin de tener completa la representación técnica del proyecto que habrá de desarrollarse en la materia.

Las actividades y prácticas que se desarrollen por el alumno(a) para esta unidad deben realizarse de manera cooperativa y colaborativa para incentivar el desarrollo de las siguientes competencias genéricas:

- Habilidades para buscar, procesar y analizar información procedente de fuentes diversas.
- Capacidad de trabajo en equipo.
- Compromiso ético.
- Compromiso con la calidad.
- Habilidad para trabajar en forma autónoma.
- Habilidad de uso de las tecnologías de la información y de la comunicación.
- Capacidad de comunicación oral y escrita.

En la unidad cuatro se atiende el Marco Legal que considera las normas, acuerdos y organismos que atienden los diferentes casos en el cómputo forense a nivel nacional e internacional, así también se revisan los Servicios de cómputo forense ofertados en México, además de que se considera la perspectiva futura desde el punto de vista tecnológico y legal.

Durante el desarrollo de las actividades programadas para la asignatura, es importante que el docente motive al estudiante para que adquiera conocimientos y entienda que está construyendo su hacer futuro y en consecuencia actúe de una manera profesional; de igual forma el docente debe hacer que el estudiante aprecie la importancia del conocimiento y el hábito de trabajo; desarrolle la precisión y la curiosidad de la innovación en el conocimiento, así como inculque los valores de la responsabilidad, la puntualidad, el entusiasmo, el interés, la tenacidad y la flexibilidad.

Es necesario que el docente ponga atención y cuidado en los aspectos señalados en el párrafo anterior para que el proceso de enseñanza – aprendizaje de esta asignatura promueva el establecimiento de relaciones objetivas entre los conocimientos que el estudiante va construyendo y la realidad social y profesional de su entorno.

### 3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Tecnológico Nacional de México campus San Juan del Río.  Mayo de 2024.	M.C.E. Amaya Pérez Angélica Jacqueline Lic. Flores Díaz Guadalupe Lic. Frago Cobos Minnie Ruth M.G.T.I. Hernández Pineda Ángel Iván	Reunión de Academia para el diseño de Módulo de especialidad y elaboración de programas de estudio.

### 4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Utiliza herramientas teórico – prácticas que le permitan obtener evidencia digital de los delitos cometidos a través de sistemas informáticos, que puedan ser utilizadas en un marco legal.

### 5. Competencias previas

<ul style="list-style-type: none"><li>• Identifica las diferentes vulnerabilidades en los sistemas de información y seguridad perimetral evaluando servicios y mecanismos necesarios para implementar una estrategia en la seguridad de la infraestructura Tecnológica, de acuerdo a los requisitos de la organización.</li><li>• Aplica marcos de referencia para la solución de problemas de seguridad y protección de la privacidad a través de la gestión de incidentes.</li><li>• Aplica técnicas y herramientas como medida para mitigar los riesgos y vulnerabilidades informáticas y que a su vez contribuyen al aseguramiento e integridad de la información y tecnologías en la organización.</li></ul>
---



## 6. Temario

No.	Temas	Subtemas
1	Introducción al Cómputo Forense	1.1. Definición, origen y objetivo. 1.2. Terminología del cómputo forense. 1.3. Áreas de aplicación. 1.4. Clasificación de delitos informáticos. 1.5. Dispositivos susceptibles al cómputo forense.
2	Herramientas de Cómputo Forense	2.1. Para la recolección de evidencias. 2.2. Para el monitoreo y control de equipo de cómputo. 2.3. Marcado de documentos. 2.4. Revisión de hardware. 2.5. Aplicación práctica de las herramientas en casos de uso.
3	Metodología del Cómputo Forense	3.1. Identificación del hecho delictivo. 3.2. Preparación de herramientas y técnicas. 3.3. Adquisición de evidencias digitales. <ul style="list-style-type: none"> <li>3.3.1 Equipo de cómputo.</li> <li>3.3.2 Dispositivos móviles.</li> <li>3.3.3 Dispositivos de red</li> <li>3.3.4 En la nube</li> </ul> 3.4. Preservación de la escena física y digital. 3.5. Análisis e interpretación de evidencias. 3.6. Presentación de resultados.
4	Análisis documental del Cómputo Forense	4.1. Marco Legal. <ul style="list-style-type: none"> <li>4.1.1 Normas regulatorias en México.</li> <li>4.1.2 Acuerdos y convenios internacionales.</li> <li>4.1.3 Organismos Nacionales e Internacionales.</li> </ul> 4.2. Estudios de casos reales, nacionales e internacionales. 4.3. Servicios de Cómputo forense ofertados en México. 4.4. Tendencias.

## 7. Actividades de aprendizaje de los temas

1. Introducción al cómputo Forense	
Competencias	Actividades de aprendizaje
<p><b>Específica(s):</b></p> <p>Utiliza la terminología asociada al cómputo forense como parte de su vocabulario para reconocer los elementos que lo conforman.</p> <p><b>Genéricas:</b></p> <ul style="list-style-type: none"><li>• Habilidades para buscar, procesar y analizar información procedente de fuentes diversas.</li><li>• Capacidad de trabajo en equipo.</li><li>• Compromiso ético.</li><li>• Compromiso con la calidad.</li><li>• Habilidad para trabajar en forma autónoma.</li><li>• Habilidad de uso de las tecnologías de la información y de la comunicación.</li><li>• Capacidad de comunicación oral y escrita.</li></ul>	<ul style="list-style-type: none"><li>• En la bibliografía sugerida, investigar la definición, origen y objetivo del cómputo forense, después realizar una comparación con sus compañeros.</li><li>• Construir un glosario de términos relacionados al cómputo forense, ordenados de manera alfabética.</li><li>• Identificar las áreas de aplicación del cómputo forense, describiendo brevemente estas áreas.</li><li>• Realizar un esquema donde se muestre la clasificación de los diferentes delitos informáticos.</li><li>• Elaborar una tabla con fotografías y descripción de los diferentes dispositivos relacionados al cómputo forense.</li></ul>
2. Herramientas de cómputo forense	
Competencias	Actividades de aprendizaje
<p><b>Específica(s):</b></p> <p>Aplica diferentes herramientas de cómputo forense para la obtención de evidencias digitales en un caso práctico.</p> <p><b>Genéricas:</b></p> <ul style="list-style-type: none"><li>• Habilidades para buscar, procesar y analizar información procedente de fuentes diversas.</li><li>• Capacidad de trabajo en equipo.</li><li>• Compromiso ético.</li><li>• Compromiso con la calidad.</li><li>• Habilidad para trabajar en forma autónoma.</li><li>• Habilidad de uso de las tecnologías de la información y de la comunicación.</li><li>• Capacidad de comunicación oral y</li></ul>	<ul style="list-style-type: none"><li>• Investigar diferentes herramientas para el cómputo forense que permitan recolectar evidencia, monitorizar y controlar hardware y definir su funcionamiento y estructura en un esquema gráfico.</li><li>• Conocer el funcionamiento de herramientas que le permitan recolectar y organizar evidencias digitales.</li><li>• Explicar las herramientas necesarias para la obtención y preservación de evidencias digitales interactuando en equipo.</li><li>• Comprender el funcionamiento de herramientas que le permitan explorar el hardware del equipo.</li></ul>



<p>escrita.</p>	<ul style="list-style-type: none"> <li>● Demostrar la funcionalidad de las herramientas en caso práctico.</li> <li>● Realizar prácticas de laboratorio que le permitan demostrar el uso de herramientas para la extracción, marcado y conservación de evidencias digitales aplicando herramientas de cómputo forense conocidas.</li> </ul>
<p>3. Metodología del cómputo forense</p>	
<p>Competencias</p>	<p>Actividades de aprendizaje</p>
<p>Específica(s):</p> <p>Aplica la metodología del cómputo forense para analizar y profundizar en la información con el objeto de generar conocimiento y soluciones en un caso práctico del contexto.</p> <p>Genéricas:</p> <ul style="list-style-type: none"> <li>● Habilidades para buscar, procesar y analizar información procedente de fuentes diversas.</li> <li>● Capacidad de trabajo en equipo.</li> <li>● Compromiso ético.</li> <li>● Compromiso con la calidad.</li> <li>● Habilidad para trabajar en forma autónoma.</li> <li>● Habilidad de uso de las tecnologías de la información y de la comunicación.</li> <li>● Capacidad de comunicación oral y escrita.</li> </ul>	<ul style="list-style-type: none"> <li>● Realizar una búsqueda de información de los temas y conceptos clave elaborando un mapa mental por cada fase de la metodología del cómputo forense.</li> <li>● Realizar la adquisición de evidencias digitales de los diferentes dispositivos y tecnologías.</li> <li>● Analizar en equipo los métodos y técnicas de la metodología del cómputo forense más utilizadas en la actualidad y en un foro justificar el uso de las mismas.</li> <li>● Elegir en grupo los métodos y técnicas de la metodología del cómputo forense a aplicar en el caso de estudio práctico elaborando una guía de observación.</li> <li>● Aplicar los métodos y técnicas de la metodología al caso de estudio práctico realizando un reporte en equipo donde se presentan los resultados y en plenaria compartir al grupo.</li> </ul>
<p>4. Análisis documental del cómputo forense.</p>	
<p>Competencias</p>	<p>Actividades de aprendizaje</p>
<p>Específica(s):</p> <p>Obtiene un panorama general del cómputo forense mediante el estudio de casos nacionales e internacionales, dentro de un marco legal, que le permita participar como perito forense.</p>	<ul style="list-style-type: none"> <li>● Analizar los documentos que conforman las normas regulatorias del cómputo forense en México y realiza un diagrama esquemático con los puntos de su interés, explicando por escrito y fundamentando los motivos de su elección.</li> </ul>

Genéricas:

- Capacidad de análisis y síntesis.
- Pensamiento crítico.
- Habilidades para buscar, procesar y analizar información procedente de fuentes diversas.
- Capacidad de trabajo en equipo.
- Compromiso ético.
- Habilidad para trabajar en forma autónoma.
- Habilidad de uso de las tecnologías de la información y de la comunicación.
- Capacidad de comunicación oral y escrita.
- Capacidad de argumentar con fundamentos.

- Estudiar los acuerdos y convenios entre estados, así como aquellos que son internacionales y de los que México forma parte, realizando una presentación en donde los describa y explique, en plenaria, en qué situaciones se aplican.
- Evaluar la efectividad de los acuerdos y convenios que han sido aplicados para resolver casos reales al defender, en un debate de grupo, los resultados obtenidos en su aplicación.
- Buscar información sobre los Organismos oficiales, Nacionales e Internacionales, encargados de resolver situaciones propias del cómputo forense y realizar un vídeo en donde los describa.
- Indagar sobre los organismos privados que ofrecen servicios de cómputo forense en México, clasificarlos de acuerdo a los servicios que oferta y realizar un manual informativo que incluya esta información, además de los datos oficiales de los mismos.
- En foro, comentar la perspectiva futura del cómputo forense, en donde se consideren los aspectos digitales, avances tecnológicos, las herramientas, métodos, técnicas y los aspectos legales.

## 8. Práctica(s)

Las prácticas han sido consideradas dentro de las actividades de aprendizaje:

- Aplicar herramientas para la obtención, análisis y preservación de evidencias digitales que sean utilizadas en el cómputo forense.
- Aplicar los métodos y técnicas de la metodología al caso de estudio práctico, realizando un reporte en equipo donde se presenten los resultados y en plenaria compartir al grupo.
- Aplicar los temas del marco legal para realizar lo siguiente:
  - Presentación que describe los convenios y acuerdos nacionales e internacionales.

- Debate en donde se evalúa la efectividad de acuerdos y convenios, en casos reales, de acuerdo a los resultados obtenidos.
- Vídeo que describe los Organismos oficiales, Nacionales e Internacionales, encargados de resolver situaciones de cómputo forense.
- Manual informativo con los organismos privados que ofrecen servicios de cómputo forense en México.
- Foro sobre la perspectiva futura del cómputo forense.

## 9. Proyecto de asignatura

El objetivo del proyecto que planteé el docente que imparta esta asignatura, es demostrar el desarrollo y alcance de la(s) competencia(s) de la asignatura, considerando las siguientes fases:

- **Fundamentación:** marco referencial (teórico, conceptual, contextual, legal) en el cual se fundamenta el proyecto de acuerdo con un diagnóstico realizado, mismo que permite a los estudiantes lograr la comprensión de la realidad o situación objeto de estudio para definir un proceso de intervención o hacer el diseño de un modelo.
- **Planeación:** con base en el diagnóstico en esta fase se realiza el diseño del proyecto por parte de los estudiantes con asesoría del docente; implica planificar un proceso: de intervención empresarial, social o comunitario, el diseño de un modelo, entre otros.
- **Ejecución:** consiste en el desarrollo de la planeación del proyecto realizada por parte de los estudiantes con asesoría del docente, es decir en la intervención (social, empresarial), o construcción del modelo propuesto según el tipo de proyecto, es la fase de mayor duración que implica el desempeño de las competencias genéricas y específicas a desarrollar.
- **Evaluación:** es la fase final que aplica un juicio de valor en el contexto laboral-profesión, social e investigativo, ésta se debe realizar a través del reconocimiento de logros y aspectos a mejorar, se estará promoviendo el concepto de “evaluación para la mejora continua”, la metacognición, el desarrollo del pensamiento crítico y reflexivo en los estudiantes.

## 10. Evaluación por competencias

La evaluación debe ser continua y formativa por lo que se debe considerar el desempeño en cada una de las actividades de aprendizaje, haciendo especial énfasis en obtener evidencias tales como:

- Informe de las actividades de búsqueda de información hechas durante las actividades realizadas en cada unidad académica, así como de las conclusiones obtenidas de las mismas.
- Descripción de otras experiencias concretas que se obtendrán al participar en discusiones, exposiciones o cualquier otro medio didáctico-profesional que trate sobre

la materia y que deberán realizarse durante el curso académico.

- Exámenes teórico-prácticos para comprobar la efectividad del estudiante en la comprensión de aspectos teóricos y su aplicación a la solución de casos de estudio prácticos.
- Reporte de detección de problemas con apoyo de herramientas de cómputo forense. Construcción de una solución de cómputo forense para un caso de estudio práctico.
- Para verificar el nivel del logro de las competencias del estudiante se recomienda utilizar: Listas de cotejo, rúbricas, listas de verificación, guías de observación, exámenes prácticos, entre otros.

## 11. Fuentes de información

Impresas:

ACISSI. (2011). Seguridad informática Ethical Hacking . Conocer el ataque para una mejor defensa (ENI ed.). España.

Arnedo P. (2014). Herramientas de Análisis Forense. y su aplicabilidad en la investigación de delitos informáticos.

Cano. (2013). Computación Forense. Descubriendo los rastros informáticos.Ed. Alfaomega.

Hidalgo I., Yasaca Saul & Hidalgo Byron (2019). Evidencias Digitales en la Investigación Informática. Editorial Politécnica ESPOCH .

Iglesias L. (2015). Herramientas OpenSource para Informática Forense. Universidad de Buenos Aires. Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Montenegro, D. B. (2015). El delito informático y su clasificación. UNIANDES EPISTEME: Revista de Ciencia, Tecnología e Innovación.

Poder Judicial de la Federación. (2016). Lineamientos para la obtención y tratamiento de los recursos informáticos y/o evidencias digitales. México: Consejo de la Judicatura.

Rodríguez, F., & Doménech, A. (2013). Informática forense: el rastro digital del crimen. Recuperado el 22 de Junio de 2020, de Dialnet-ElRastroDigitalDelCrimen-3740775.pdf  
SEGOB. (17 de Junio de 2016). Acuerdo General del Pleno del Consejo de la Judicatura Federal, por el que se expide el Protocolo de actuación para la obtención y tratamiento de los recursos informáticos y/o evidencias digitales. Diario Oficial de la Federación .

Electrónicas:

Agencia de Investigación Criminal. (Junio de 2018). Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas. Recuperado el 22 de Junio de 2020, de Guía técnica de cadena de custodia de evidencia digital:  
[http://www.coahuilatrasmis.gob.mx/disp/documentos\\_disp/GU%C3%8DA%20T%C3%89CNICA%20DE%20CADENA%20DE%20CUSTODIA%20DE%20EVIDENCIA%20DIGITAL.pdf](http://www.coahuilatrasmis.gob.mx/disp/documentos_disp/GU%C3%8DA%20T%C3%89CNICA%20DE%20CADENA%20DE%20CUSTODIA%20DE%20EVIDENCIA%20DIGITAL.pdf)



Cano, J. (2010). Introducción a la Informática forense, una disciplina técnico-legal. Recuperado el 22 de Junio de 2020, de [http://acistente.acis.org.co/typo43/fileadmin/Revista\\_96/dos.pdf](http://acistente.acis.org.co/typo43/fileadmin/Revista_96/dos.pdf)

López D. Análisis Forense Digital, obtenido de [https://oas.org/juridico/spanish/cyb\\_analisis\\_foren.pdf](https://oas.org/juridico/spanish/cyb_analisis_foren.pdf)

Pino, S. A. (2010). Delitos informáticos: Generalidades. Recuperado el 22 de junio de 2020, de [https://www.oas.org/juridico/spanish/cyb\\_ecu\\_delitos\\_inform.pdf](https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf)

#### ENLACES PARA DESCARGA DE SOFTWARE PARA PRÁCTICAS:

EXTERRO, Plataforma de software para descubrimiento y gobernanza de la información: <https://www.exterro.com/ftk-imager>

AUTOPSY DIGITAL FORENSICS, Plataforma forense digital de código abierto: <https://www.autopsy.com/>

BELKASOFT, Software de identificación de documentos falsificados: <https://belkasoft.com/>

CYBERDEFENDERS, Plataforma de entrenamiento enfocado al desarrollo de habilidades de ciberdefensa: <https://cyberdefenders.org/>